A Secure Collaboration System for Coal Supply Chains in Australia

Shiping Chen and **Chen Wang**

Information Engineering Lab
CSIRO ICT Centre, Australia

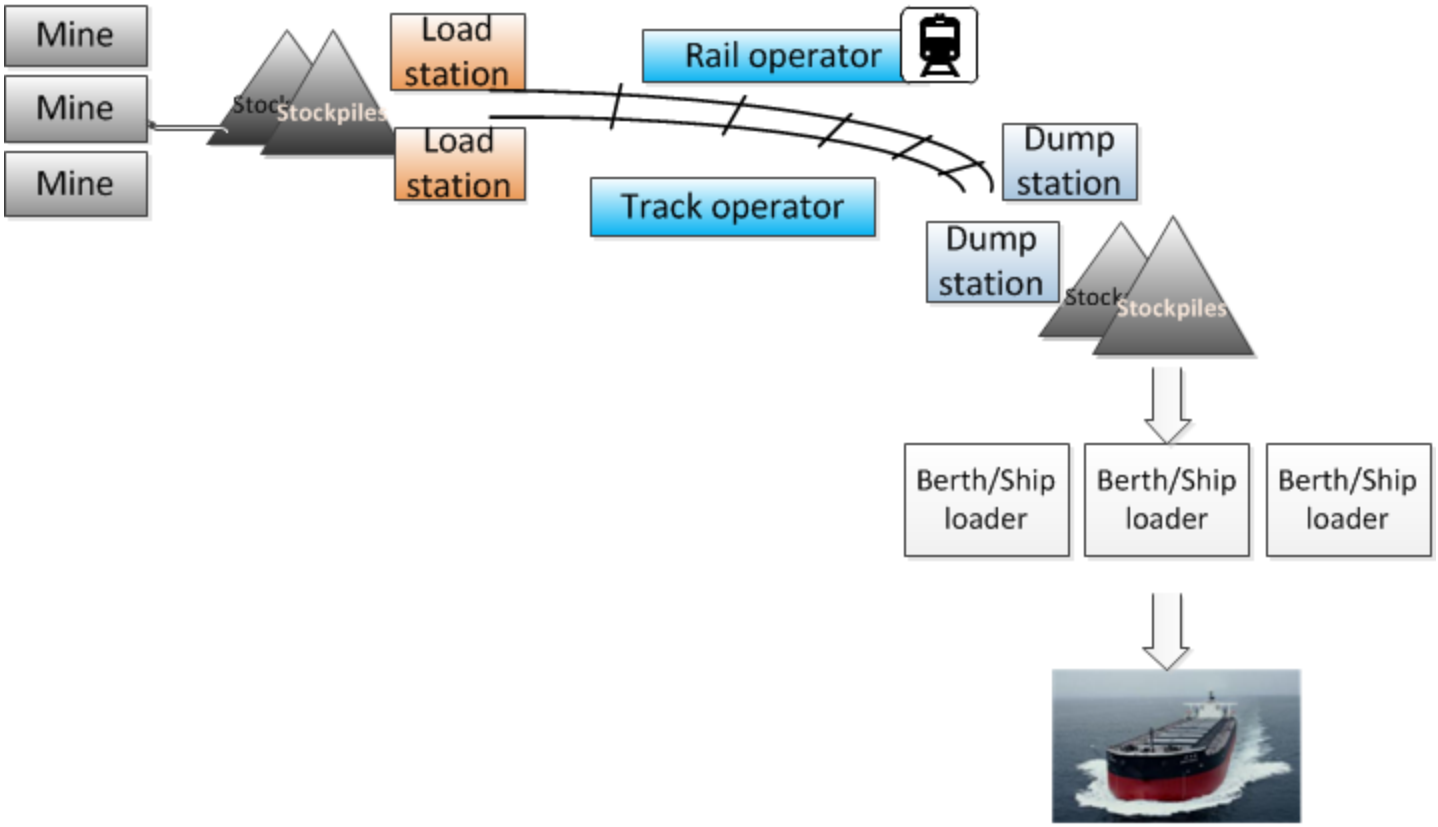
Microsoft Cloud Futures 2011, June 3

CSIRO

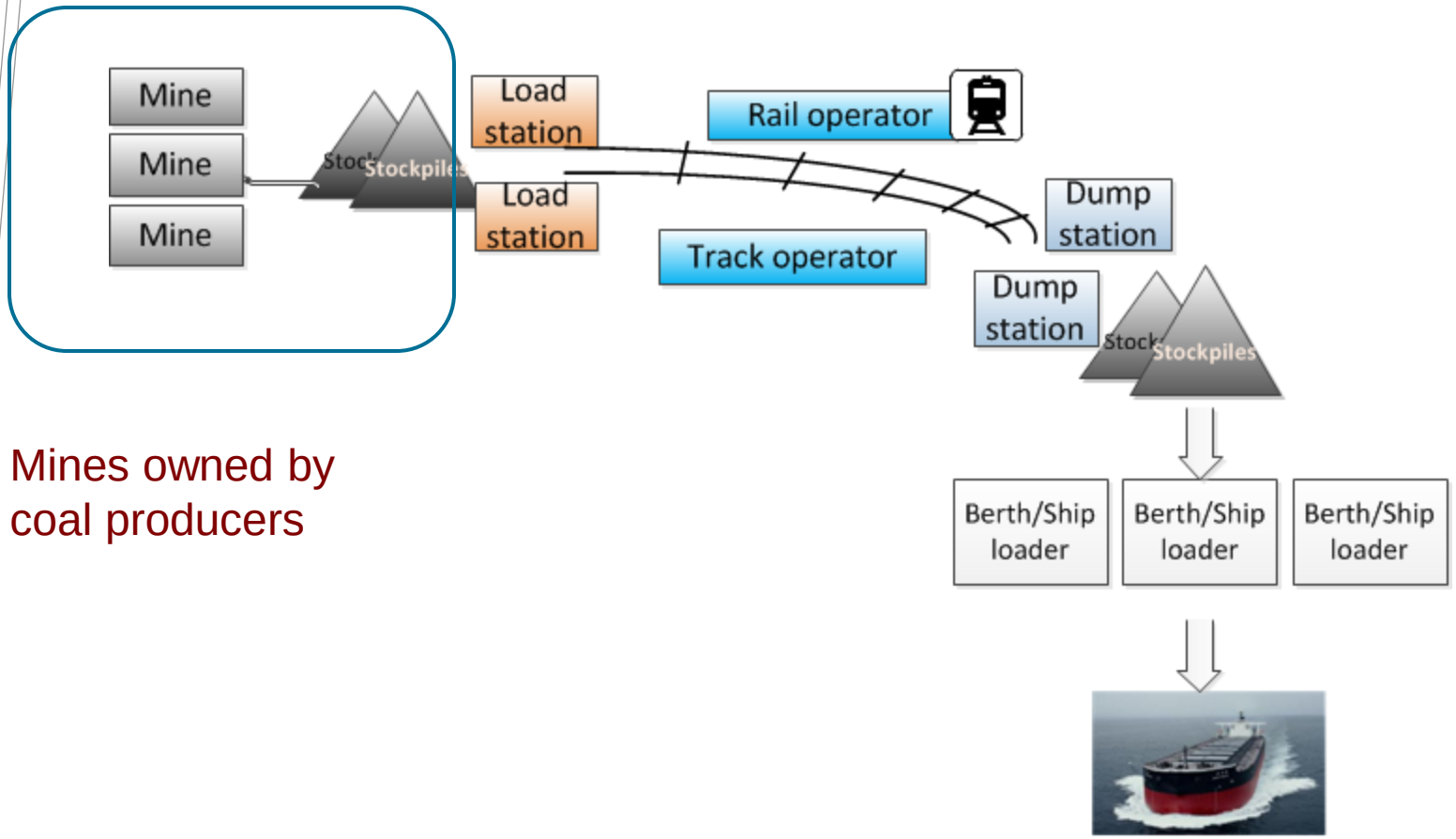
Outlines

- Background of Coal Chains
- Challenge for Collaboration in Coal Chains
- Information Flow Control Mechanism
- The Role of “Cloud” in Information Flow Control
- Conclusion

Coal Supply Chain Example

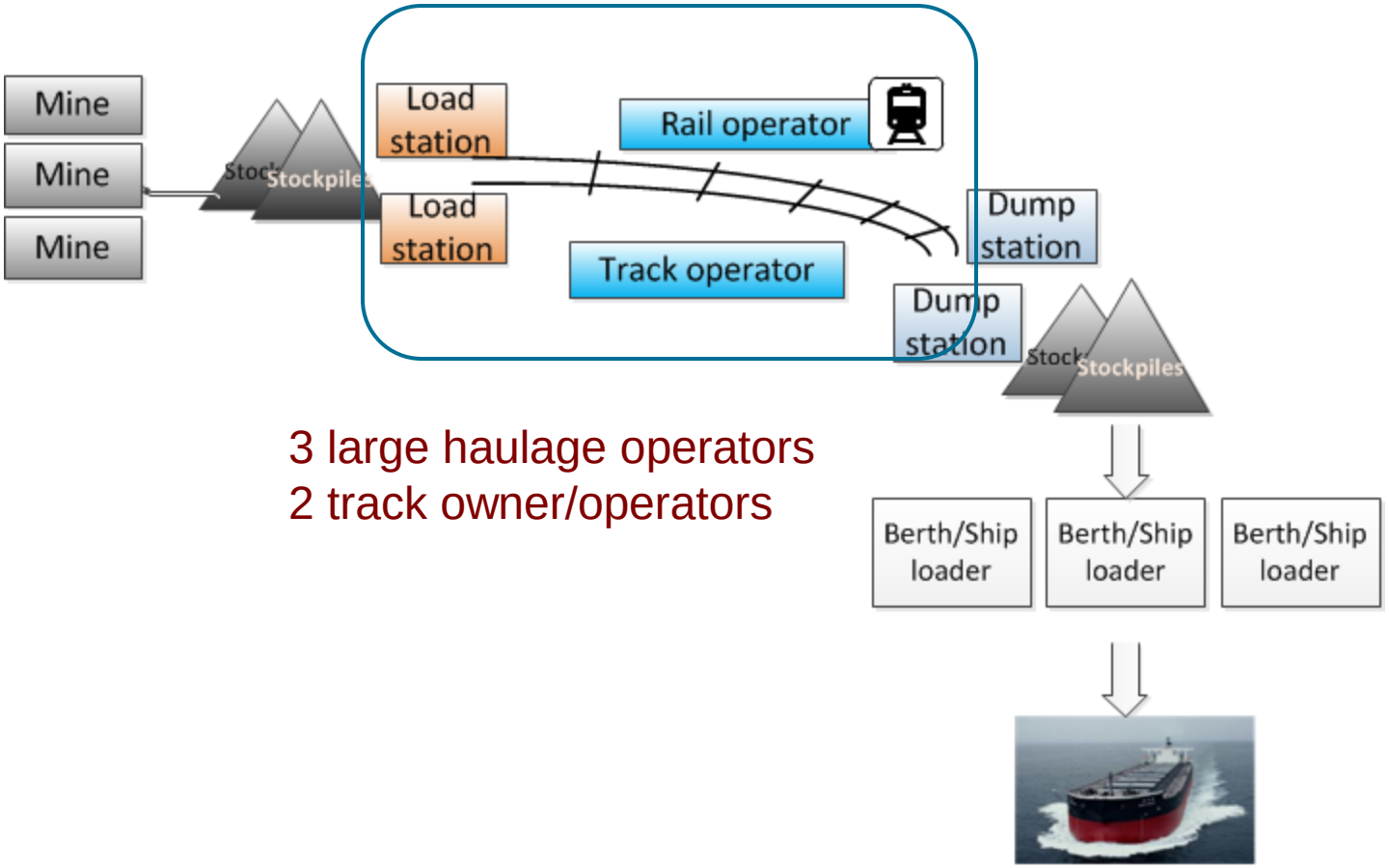


Coal Supply Chain Example



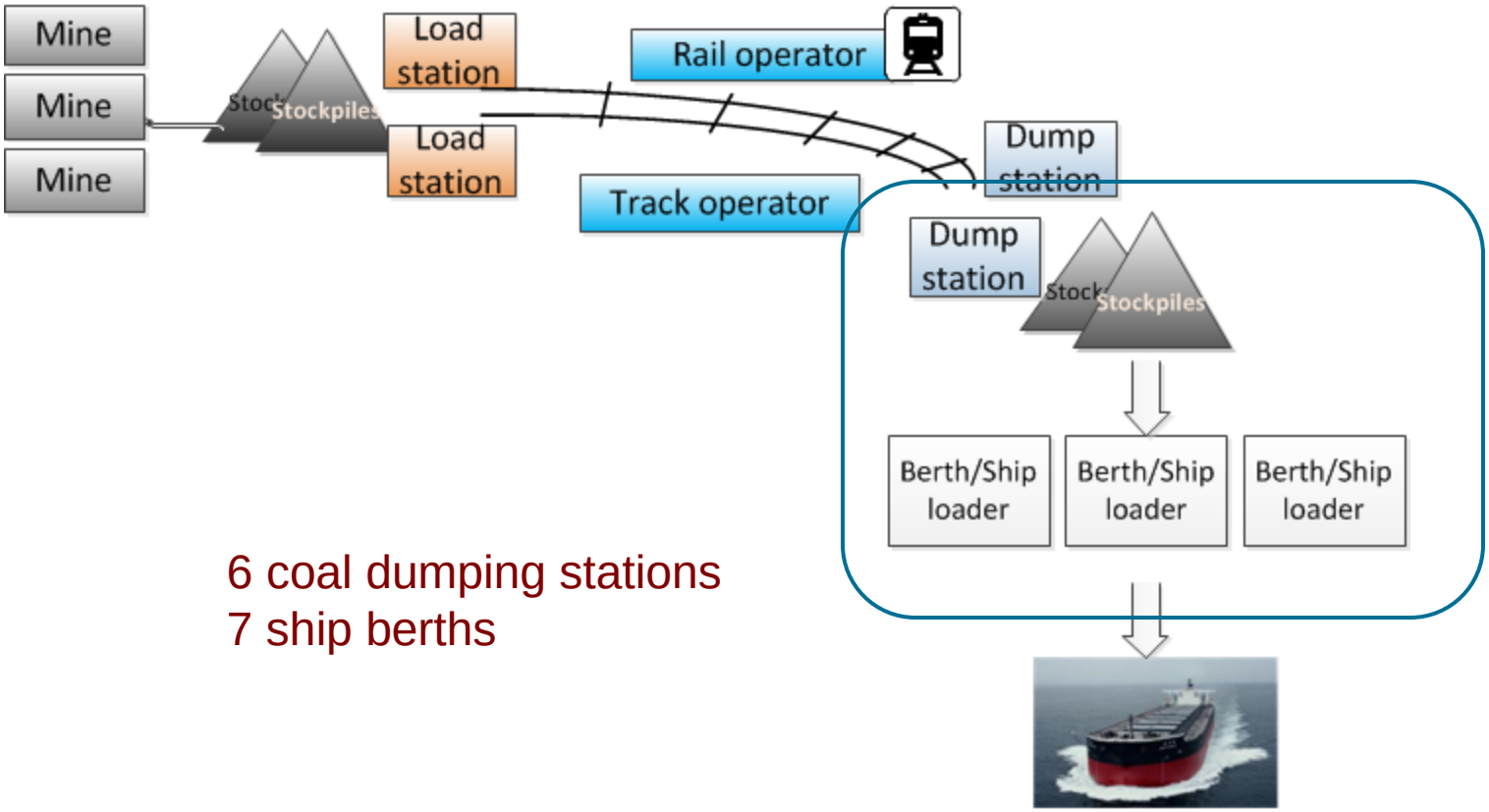
40 Mines owned by
13 coal producers

Coal Supply Chain Example



3 large haulage operators
2 track owner/operators

Coal Supply Chain Example



6 coal dumping stations
7 ship berths

CSIRO

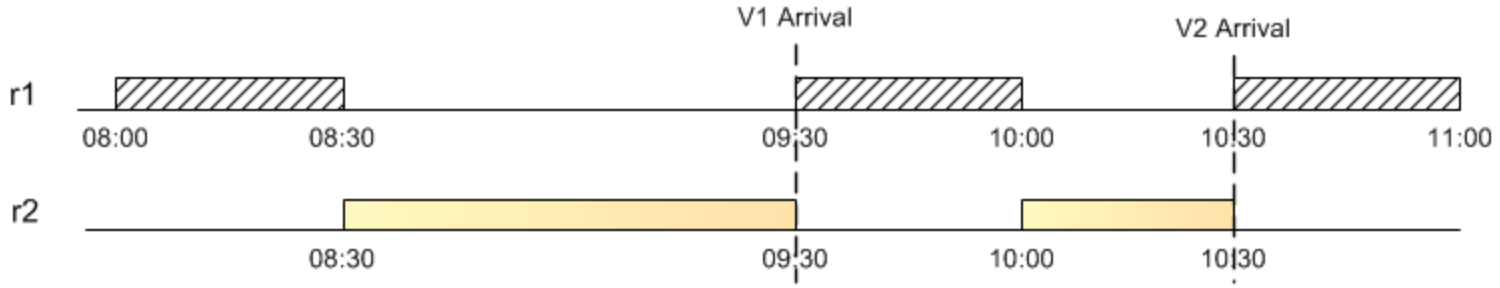
The Need of Coordination in Coal Chain

- A typical transport supply chain in Australian coal industry involves multiple business entities that own different resources
  - Hunter Valley Coal Chain: 40 coal mines owned by 13 producers, 27 load points, 28 trains run by 3 rail operators, tracks own by 2 operators, 3 coal loading terminals, 7 ship berths, 9 vessel agents, 34 end buyers from 12 countries…
- The producers and operators are independent organizations
  - They contract with each other to ensure the resources for shipping the coal.
  - Owners of same type of resources compete with each other.
- Problems
  - Individually negotiated contracts may not lead to an optimal (or sometimes even feasible) resource usage in the whole coal chain.

CSIRO

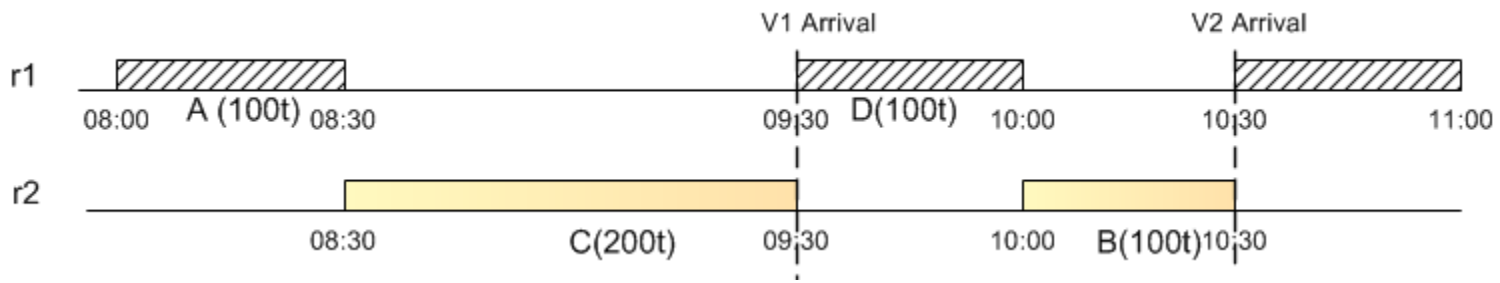
The Need of Coordination in Coal Chain

- Two vessels ship different brands of coals from the same berth
  - V1: (100 tones: mine A, 100 tones: mine B); arrives at 9:30
  - V2: (200 tones: mine C, 100 tones: mine D); arrives at 10:30
- Miners negotiate with rail operators independently for shipping coals to the berth
  - Miner A, D negotiate with Rail Operator r1
  - Miner B, C negotiate with Rail Operator r2
- Rail Operator r1 and r2 contract with track operator T for track allocation



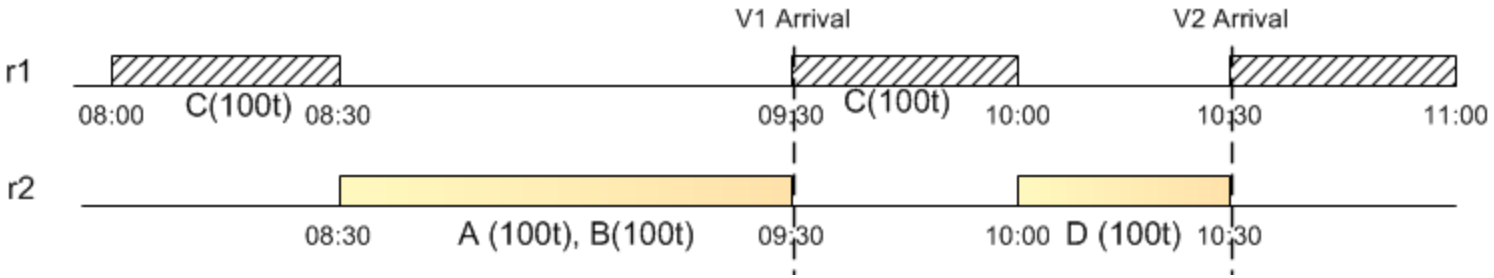
The Need of Coordination in Coal Chain

- Schedule 1



  - Vessel waiting time: v1 – 1 hour; v2 – 0.5 hour

- Schedule 2

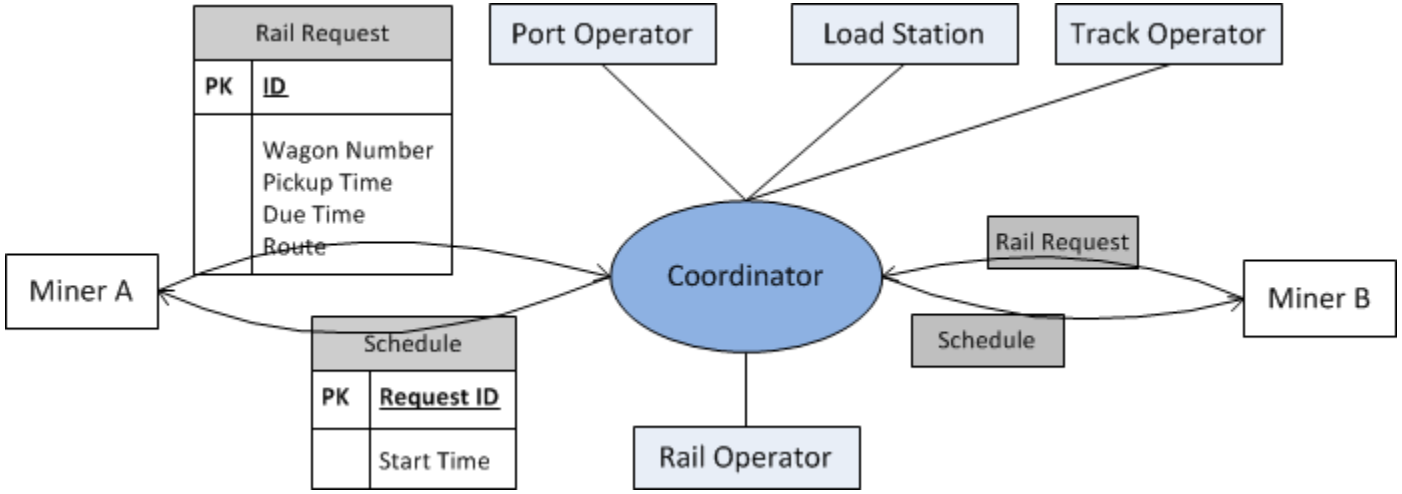


  - Vessel waiting time: v1 – 0 hour; v2 – 0 hour

CSIRO

Challenges for Sharing Data in Coal Chain

- The coal chain can run more efficiently with a coordinator



- The obstacle of setting up a coordinator
  - miners or operators need to make some sensitive information available to the coordinator,
    - e.g., Miner A needs to disclose to the coordinator that it needs to transport *100* tones coal to stockyard 1 for loading to vessel *v1* that arrives at 9:30.
  - The current coal chain practices do not guarantee that the information won't flow to the competitors of the information provider.
  - Convincing miners and operators to share information is difficult.

CSIRO

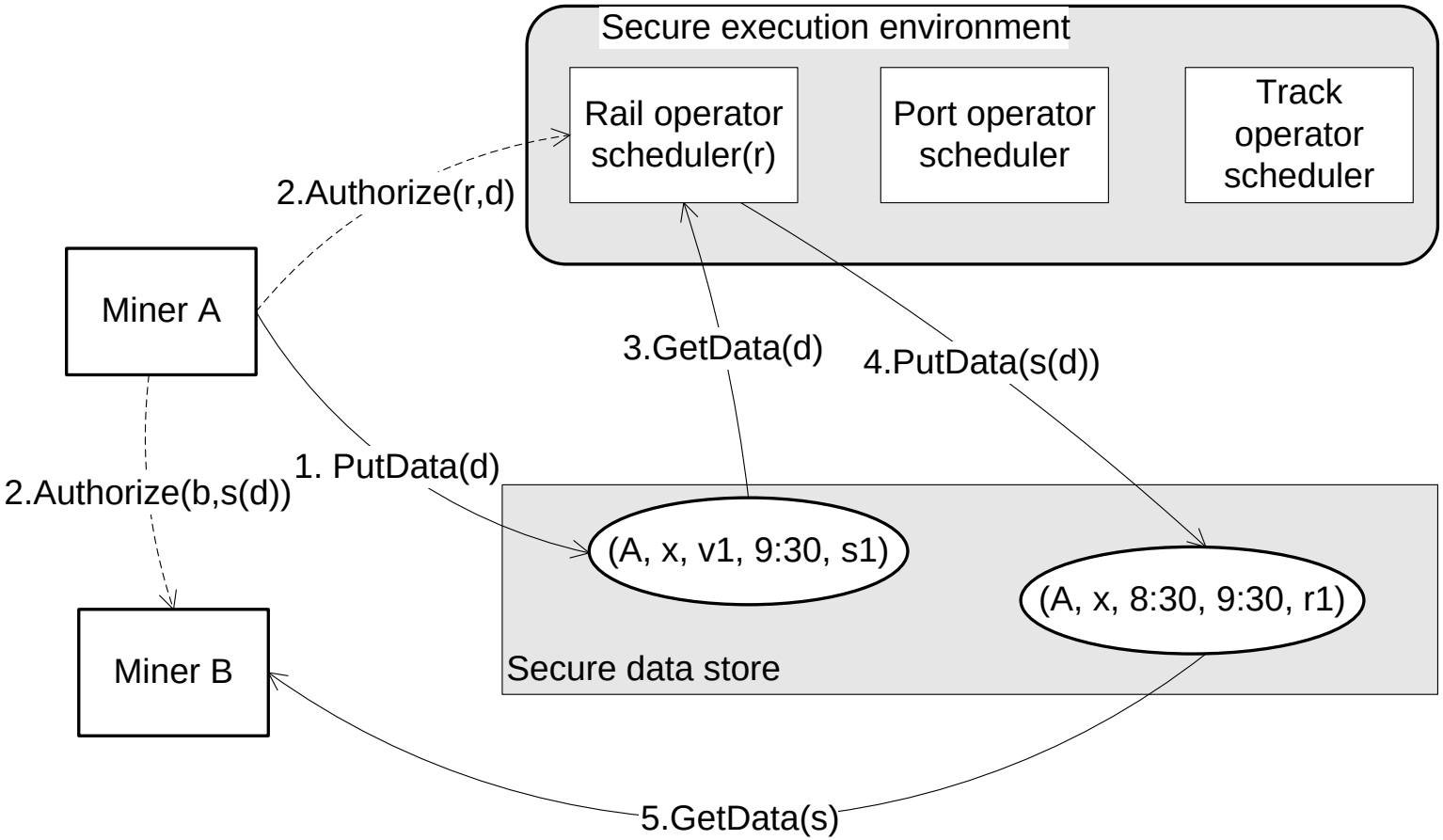
System Requirement

- The system should ensure that shared information is only used for the purpose specified by the information provider
  - The system should allow the party that supplies the data to specify who can use the data and how the data should be used;
  - The owner specified policies should be enforced when data flow across administrative boundaries;
  - A user-supplied program that accesses a set of data in the system should label information flow inside the program
    - For checking if the program satisfies the access control and information flow policies of its data owner.
    - The access to the output produced by an application from a set of data should also satisfy certain policies specified by the owners of input data.

Information Flow Control

- The system shall consist of the following components in order to meet the requirements:
  - A secure data store
    - Only allows authorized parties to access data according to the access control policies specified by the data owner.
    - Enforces information flow control policies.
  - A secure execution environment
    - Provides a mechanism to ensure that user-supplied programs follow information flow policies associated with data they access.
    - Provides isolation mechanism for running user-supplied programs..

Information Flow Control: Example

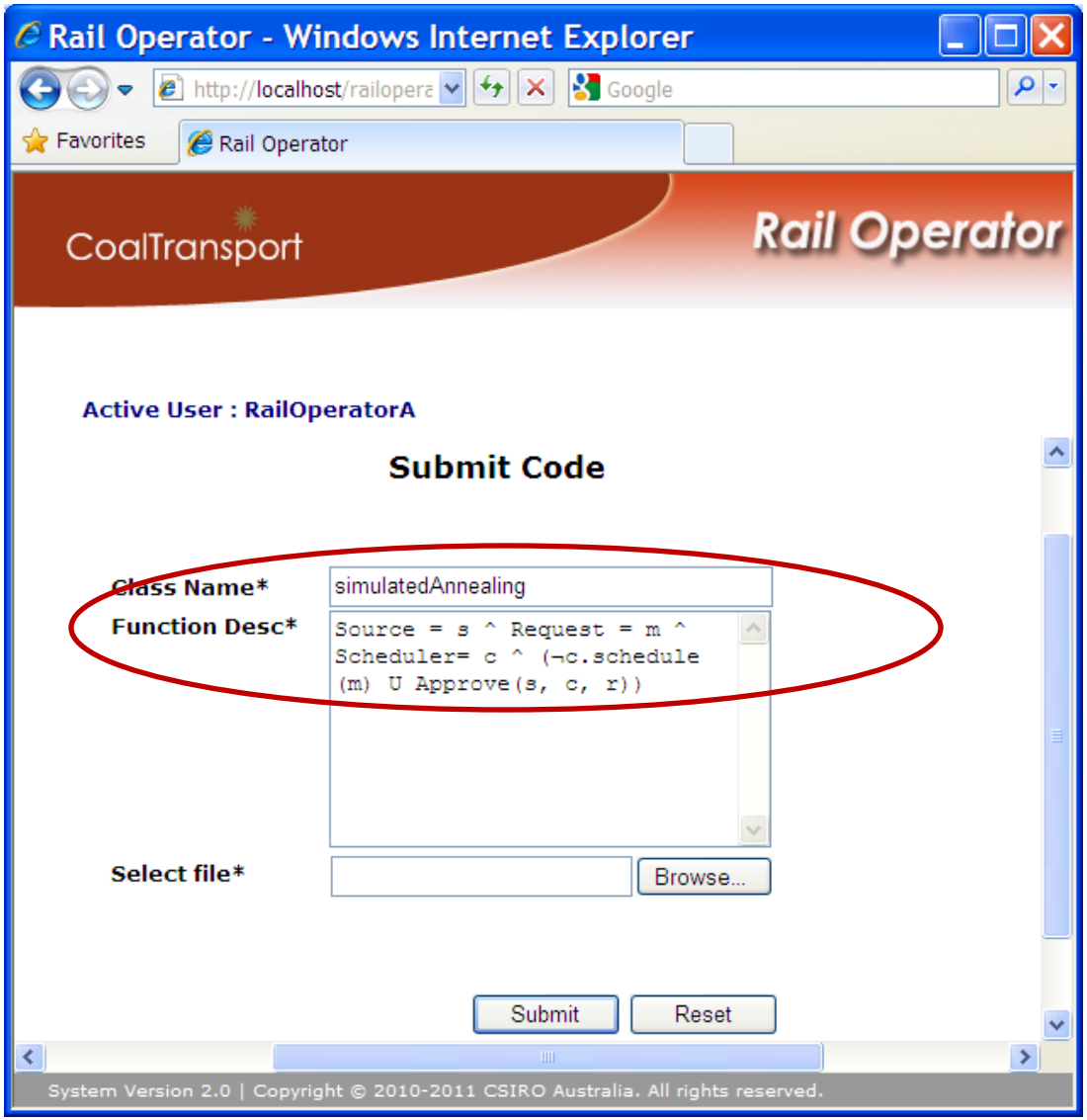


LTL based Data Labelling

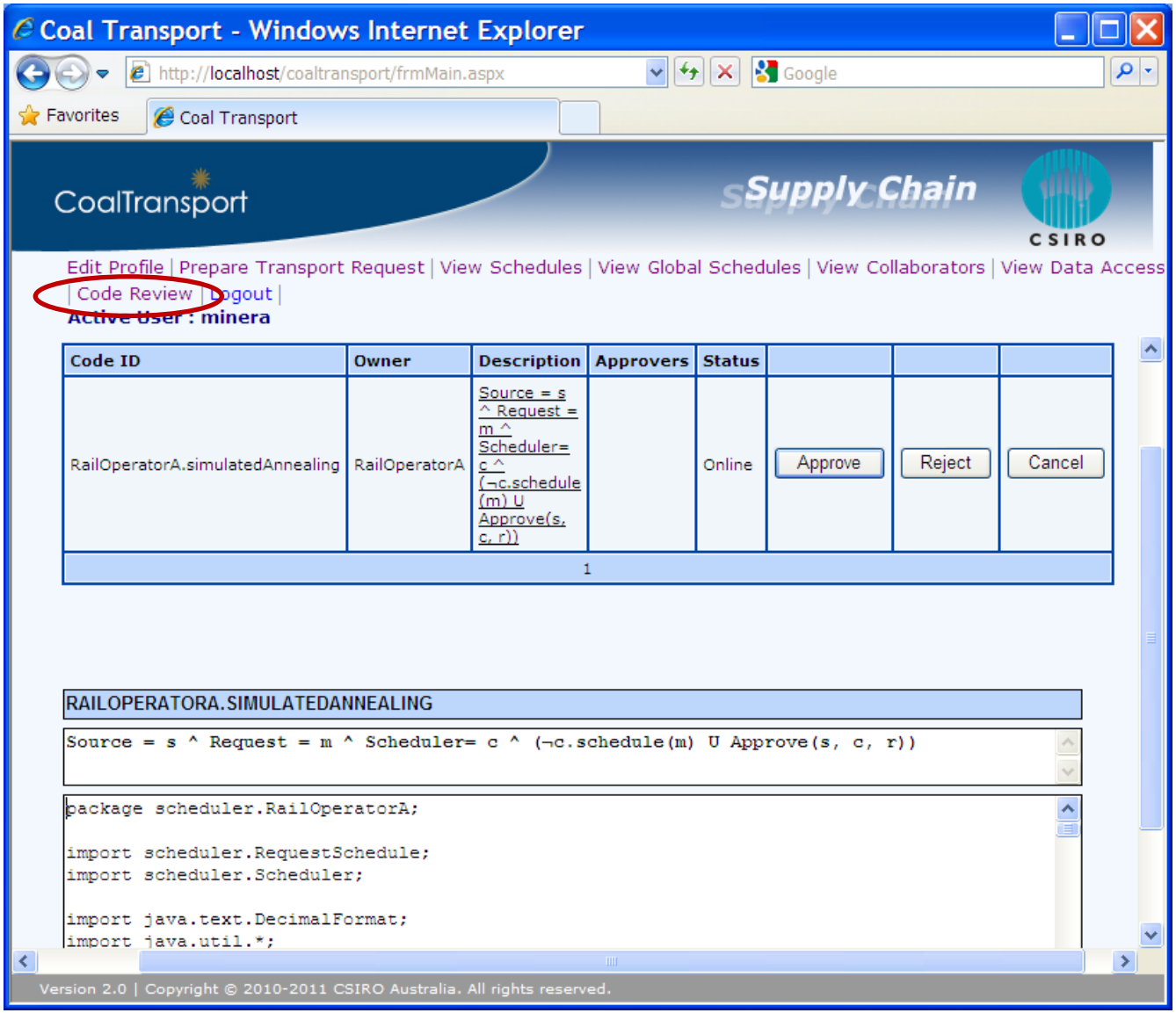
- Request is not allowed to propagate to a party without the approval from the owner
  - Source = s ^ Request = m ^ Target = t ^ (¬(r → t) **U** Approve(s, t, m))
- A scheduler cannot process a request without approval from the owner
  - Source = s ^ Request = m ^ Scheduler= c ^ (¬c.schedule(m) **U** Approve(s, c, r))
- The scheduler output cannot flow to a party without the approval from the owner
  - Source = s ^ Request = m ^ Scheduler= c ^ Target = t ^ (¬c.schedule(m) → t **U** Approve(s, c.schedule(m), t))

CSIRO

Rail operator – submit code

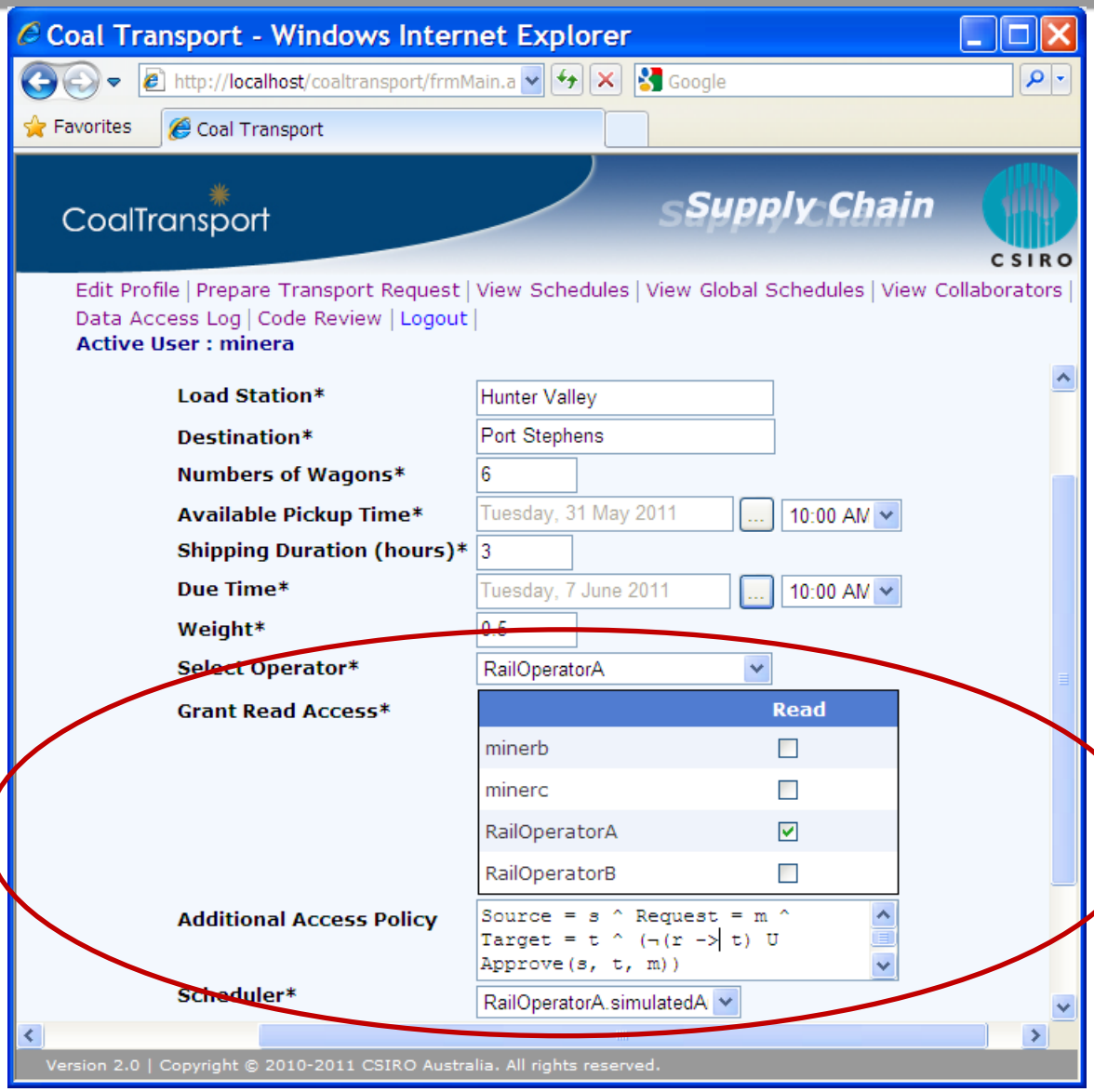


Miner – review the code accessing the data



CSIRO

Miner – submit and label request



CSIRO

Limitation of Information Flow Control

- Who plays the coordinator's role?
  - It is difficult to setup an independent party for the coordinating process.
  - It is technically challenging to manage and maintain a secure execution environment and a secure data store.
- Threats
  - Software bugs
  - Inside attack: the coordinator is formed by stakeholders
    - Tamper execution environment
    - Leak data from the store

Accountability

"People think that security in the real world is based on locks. In fact, realworld security depends mainly on deterrence, and hence on the possibility of punishment."

Butler Lampson: "Privacy and security - Usable security: how to get it." CACM 52(11), 2009

"Accountability is the ability to hold an entity, such as a person or organization, responsible for its actions."

Butler Lampson:"Accountability and Freedom", 2005

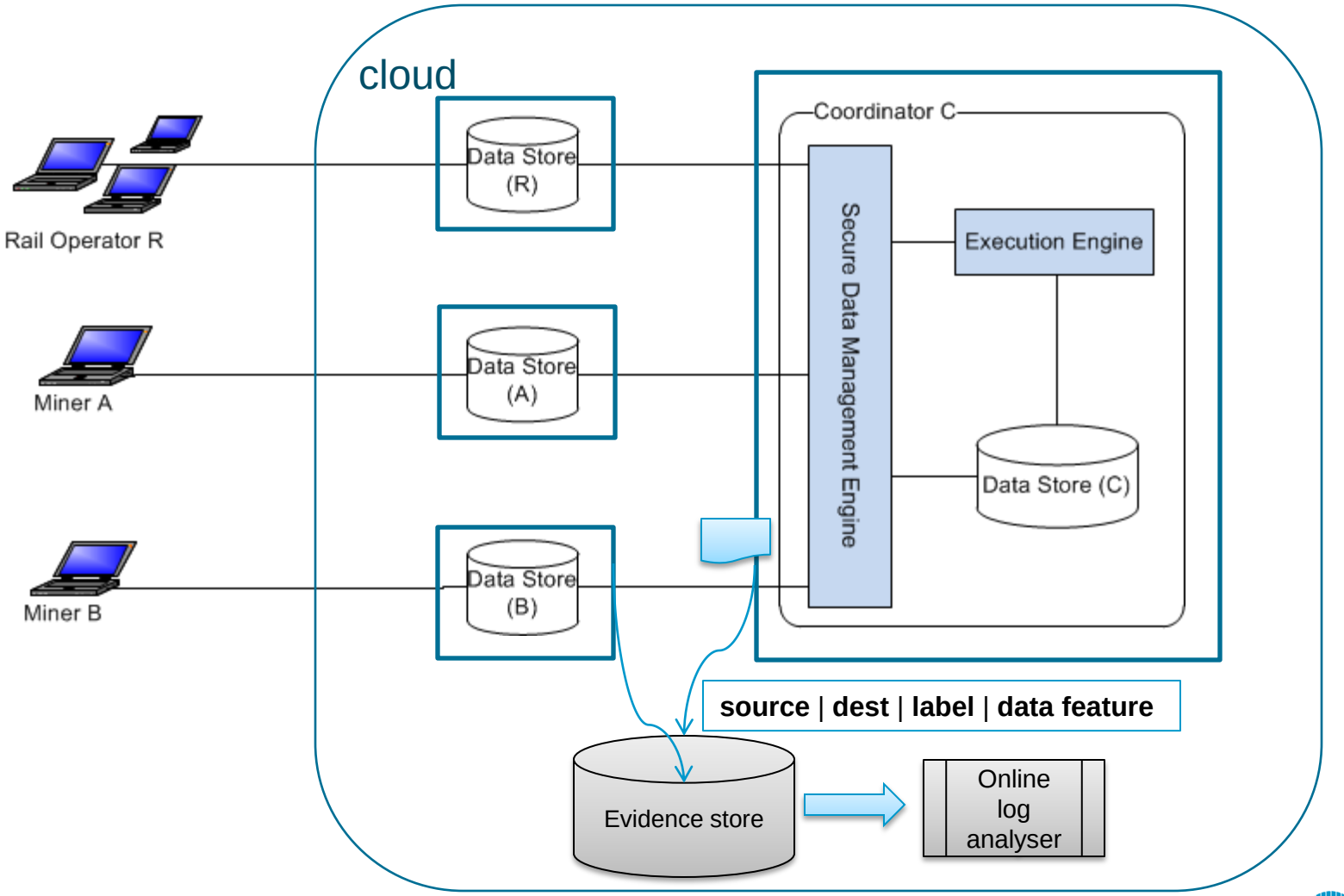
CSIRO

The Role of “Cloud”

- Accountability in business world
  - The use of a trusted third party to make a deal
  - The use of legal/social systems
    - Contract law provides incentives that promote good behaviour between parties
- Using the “cloud” as a middleman if the cloud provider is more trustworthy for a party than its collaborative parties
  - Execution environment of each party is isolated in the cloud.
  - Data and program labels describing how information may flow is visible by the “cloud”.
    - A party can be caught accountable by the “cloud” when violating the information flow policy.
  - The middleman’s role
    - Evidence collection based on disclosed policies associated with data and programs
    - Runtime compliance check and problem detection

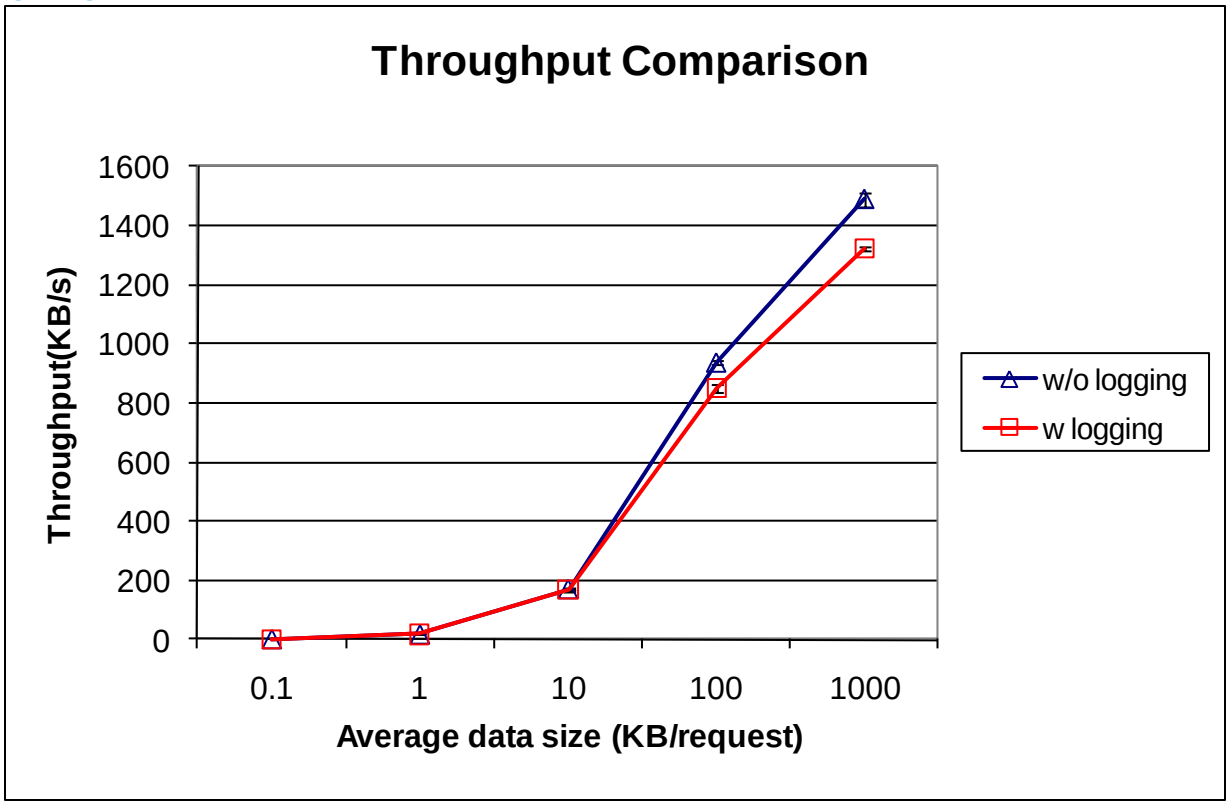
CSIRO

Coal Supply Chain in the Cloud



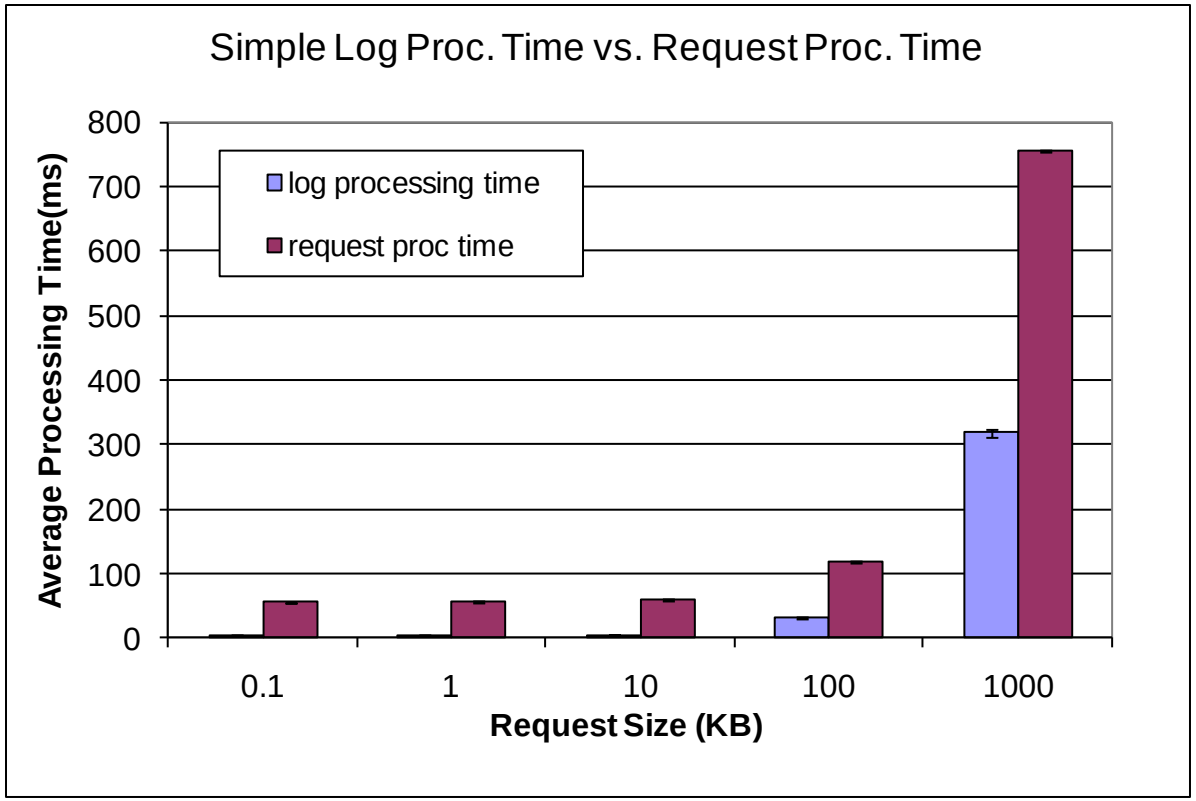
Preliminary Performance Evaluation

- Amazon EC2 small instances
  - Simple storage service (put/get)
  - Tomcat + axis2 + BerkeleyDB XML
- Logging overhead



Preliminary Performance Evaluation

- SOAP Message Reconstruction Cost



Conclusion

- Data sharing in business collaborations is difficult even for achieving common benefit
  - Collaborating parties often competing with each other at the same time
  - Information flow control alone cannot address this problem
- The cloud computing paradigm offers opportunities to solve the problem
  - Cloud computing technologies provide effective isolation for data and compute of collaborating parties.
  - An independent cloud infrastructure provider creates a middleman's role even though cloud platform itself has trustworthiness problem
    - capable of collecting evidences based on interactions between collaborating parties.